FORM PTO-1390 REV. 5-93	US DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEYS DOCKET NUMBER P01,0133
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		U.S.APPLICATION NO. (if known, see 37 CFR 1.5) 09/807129
INTERNATIONAL APPLICATION NO. **PCT/EP99/07329**	INTERNATIONAL FILING DATE 4 October 1999	PRIORITY DATE CLAIMED 6 October 1998

TITLE OF INVENTION
"METHOD FOR OPERATING A COMPUTER WITH COPY PROTECTION FOR USER PROGRAMS"

APPLICANT(S) FOR DO/EO/US
Hartwig SCHWIER and Thomas MATHIESEN

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay.
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. §371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).)
10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C.371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98; **(PTO 1449, Prior Art, Search Report).**
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included. **(SEE ATTACHED ENVELOPE)**
13. ☒ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☒ A substitute specification & marked up version of application.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information:
    a. ☒ Submittal of Drawings
    b. ☒ **EXPRESS MAIL #EL 843728464US, dated April 6, 2001.**

U.S. APPLICATION NO. (if known, see 37 C.F.R. 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/807129	PCT/EP99/07329	P01,0133

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 C.F.R. 1.492(a)(1)-(5): Search Report has been prepared by the EPO or JPO $860.00		
International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) .. $700.00		
No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C.F.R. 1.445(a)(2) $770.00		
Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee (37 C.F.R. 1.445(a)(2) paid to USPTO $1040.00		
International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) ..... $ 96.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 C.F.R. 1.492(e)).	$	

Claims	Number Filed	Number Extra	Rate		
Total Claims	11 - 20 =		X $ 18.00	$	
Independent Claims	1 - 3 =		X $ 80.00	$	
Multiple Dependent Claims			$270.00+	$	
TOTAL OF ABOVE CALCULATIONS =				$ 860.00	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 C.F.R. 1.9, 1.27, 1.28)				$	
SUBTOTAL =				$ 860.00	
Processing fee of $130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$ 860.00	
Fee for recording the enclosed assignment (37 C.F.R. 1.21(h). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). $40.00 per property +					
TOTAL FEES ENCLOSED =				$ 860.00	
				Amount to be refunded	$
				charged	$

a. ☒ A check in the amount of $ 860.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. **501519**. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Schiff Hardin & Waite
Patent Department
6600 Sears Tower
Chicago, Illinois 60606

CUSTOMER NO. 26574

SIGNATURE

Melvin A. Robinson
NAME

31,870
Registration Number

JC08 Rec'd PCT/PTO 06 APR 2001

FORM PTO-1390 REV. 5-93	US DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEYS DOCKET NUMBER
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		P01,0133
		U.S.APPLICATION NO. (if known, see 37 CFR 1.5) 09/807129

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP99/07329	4 October 1999	6 October 1998

TITLE OF INVENTION
"METHOD FOR OPERATING A COMPUTER WITH COPY PROTECTION FOR USER PROGRAMS"

APPLICANT(S) FOR DO/EO/US
Hartwig SCHWIER and Thomas MATHIESEN

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay.
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. §371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).)
10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C.371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98; **(PTO 1449, Prior Art, Search Report)**.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included. **(SEE ATTACHED ENVELOPE)**
13. ☒ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☒ A substitute specification & marked up version of application.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information:
    a. ☒ Submittal of Drawings
    b. ☒ **EXPRESS MAIL #EL 843728464US, dated April 6, 2001.**

JC08 Rec'd PCT/PTO 06 APR 2001

U.S. APPLICATION NO. (If known, see 37 CFR 1.5) 09/807129	INTERNATIONAL APPLICATION NO. PCT/EP99/07329	ATTORNEY'S DOCKET NUMBER P01,0133

17. ☒ The following fees are submitted:

	CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 C.F.R. 1.492(a)(1)-(5): Search Report has been prepared by the EPO or JPO $860.00		
International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) .. $700.00		
No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C.F.R. 1.445(a)(2) $770.00		
Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee (37 C.F.R. 1.445(a)(2) paid to USPTO $1040.00		
International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) ..... $ 96.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 C.F.R. 1.492(e)).	$	

Claims	Number Filed	Number Extra	Rate		
Total Claims	11 - 20 =		X $ 18.00	$	
Independent Claims	1 - 3 =		X $ 80.00	$	
Multiple Dependent Claims			$270.00 +	$	
TOTAL OF ABOVE CALCULATIONS =				$ 860.00	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 C.F.R. 1.9, 1.27, 1.28)				$	
SUBTOTAL =				$ 860.00	
Processing fee of $130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$ 860.00	
Fee for recording the enclosed assignment (37 C.F.R. 1.21(h). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). $40.00 per property +					
TOTAL FEES ENCLOSED =				$ 860.00	
				Amount to be refunded	$
				charged	$

a. ☒ A check in the amount of $ 860.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. **501519**. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Schiff Hardin & Waite
Patent Department
6600 Sears Tower
Chicago, Illinois 60606

CUSTOMER NO. 26574

SIGNATURE

Melvin A. Robinson
NAME

31,870
Registration Number

BOX PCT

IN THE UNITED STATES DESIGNATED OFFICE

OF THE UNITED STATES PATENT AND TRADEMARK OFFICE

UNDER THE PATENT COOPERATION TREATY-CHAPTER II

PRELIMINARY AMENDMENT

APPLICANT(S): HARTWIG SCHWIER ET AL

ATTORNEY DOCKET NO. P01,0133

INTERNATIONAL APPLICATION NO: PCT/EP99/07329

INTERNATIONAL FILING DATE: 4 OCTOBER 1999

INVENTION: METHOD FOR OPERATING A COMPUTER WITH COPY PROTECTION FOR USER PROGRAMS

Assistant Commissioner for Patents

Washington, D.C. 20231

In the Specification:

Amend the specification as follows:

SPECIFICATION

TITLE

"METHOD FOR OPERATING A DATA PROCESSING SYSTEM WITH COPY PROTECTION FOR USER PROGRAMS"

Field of the Invention

The present invention is directed to a method for operating a data processing system with copy protection for user programs.

Description of the Related Art

The production of user programs requires considerable development time and specific know how; it is therefore relatively involved. User programs are often loaded onto storage media, for example on CDROMs, and supplied to the user in this condition. Such storage media are relatively inexpensive and are unrelated to the economic outlay that is incurred in the production of the user program. It is not only relatively easy to make legal backup copies of such storage media with traditional data processing systems, but pirated copies of these user programs can also be easily produced and handed over to further users for a certain price or distributed in some other way. The producer of the user programs thus suffers considerable damage.

Numerous copy protection methods have been developed in order to put an end to this practice. In a widespread copy protection method, a dongle is employed that is plugged onto a parallel interface, onto a serial interface or a USB bus of a data processing system. This dongle is supplied to the user together with the user program. The dongle as well as the user program contain the same copy protection identification in the form of alphanumerical characters. The presence of the dongle and, thus, of the copy protection information, is queried either at the program start or continuously during the program operation. When an attempt is made to operate the user program without the dongle, then the program is aborted.

When there are a great number of users who require different user programs, then a dongle is to be provided for each user. One storage medium per user must then be provided, the user programs intended for this user being contained thereon and then containing the same copy

protection identification as the respective dongle. When a user orders following user programs, then the following steps are required: producing a storage medium for this user; storing the user programs requested by the user; and providing the user programs with the copy protection identification of the dongle. Such a procedure is involved both for the user as well as for the producer of such user programs. US Patent No. 5,386,369 discloses a method based on dongles.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a method for operating a data processing system with copy protection for user programs that assures a dependable copy protection, works simply and can be realized with little outlay for producer and user.

According to the invention, a method for operating a data processing system with copy protection for user programs is provided, whereby a plurality of application programs as well as an installation program and a cryptoprogram are on hand on a storage medium, when processing the installation program on the data processing system, the user inputs a copy protection identification, a user identification that identifies the user and an encrypted product identification that identifies at least one user program,each user program contains a predetermined memory area into which the copy protection identification can be entered, the installation program compares the copy protection identification that has been input to a copy protection identification connected with the data processing system and, given coincidence, deciphers the encrypted product identification upon utilization of the user identification as a key, and identifies the user program selected in the product identification, the selected user program is loaded from the storage medium into a memory area of the data processing system, the cryptoprogram enters the copy protection identification into the predetermined memory area of the selected user program, and, before the running of the selected

user program, the copy protection identification contained in the predetermined memory area is compared to the copy protection identification connected with the data processing system, and the user program is run only given coincidence.

According to the present invention, a product identification and a user identification are communicated to the user. The product identification, preferably composed of alphanumerical characters, identifies -- in encrypted form -- the user program or, respectively, a plurality of user programs purchased by the user. Further, the user identification is likewise, for example, in the form of alphanumerical characters. This user identification serves as the key for the encryption and deciphering of the product identification. With the assistance of this product identification and the user identification, only those programs that are referenced in the product identification are enabled for the user. Accordingly, one storage medium, for example a CDROM, can contain all user programs of the manufacturer of the user programs. The customer or, respectively, user, however, can only access those user programs that he actually ordered and purchased and that can be enabled for him. The copy protection with the assistance of the copy protection identification is retained, i.e. the data processing system on which the user program is run is directly connected to a copy protection identification with the assistance of a hardware module. This user program can only be run on the specified data processing system when the user program also contains this copy protection identification; otherwise, operations are aborted. In this way, even the production of pirated copies and their forwarding to other users are worthless, since this other user does not possess the matching user identification, the matching product identification and the matching copy protection identification.

In one exemplary embodiment of the invention, the product identification also contains the copy protection identification, whereby this copy protection identification is also compared to the copy protection identification connected with the data processing system, and the running of the further program steps only continues given coincidence. Usually, the copy protection identification is assigned only once. Accordingly, a copy protection for the user programs themselves is still present even if the product identification is improperly handed over to another user.

An authentification between the installation program and the key program is preferably undertaken when calling the key program, which enters the copy protection identification in predetermined memory areas of the user program. In this way, a traditional, modular key program that usually runs on standard data processing systems can be employed. Nonetheless, a protection of the key program ensues due to the authentification between key program and installation program, and an adequate protection against misuse is established.

BRIEF DESCRIPTION OF THE DRAWINGS

An exemplary embodiment of the invention is explained below on the basis of the drawing

Figure 1 is a flowchart that shows critical steps of the inventive method;

Figure 2 is the flowchart when a new user orders one or more user programs; and

Figure 3 shows the executive sequence when an old user orders user programs.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 shows the critical steps of the method on the basis of a simple flowchart. The customer or user receives a plurality of user programs from the manufacturer of these user programs on a storage medium, for example a CDROM, according to the order. The user, for example, has only ordered a specific selection of user programs and only paid for these. Nonetheless, many other

user programs, which could be of use to the user in future and of which he can definitely make security copies, are on this storage medium. Further, the user receives a dongle from the manufacturer with a copy protection identification KI_D. This dongle must be plugged onto the parallel interface of the data processing system in order to be able to run the installation program and enable a proper operation of the user program, which has yet to be installed. Further, the user receives an alphanumerical user identification AI. This user identification serves later as the key for deciphering the product identification PI that is likewise given to the user. This product identification PI, for example, is likewise composed of alphanumerical characters and contains, on the one hand, the copy protection identification KI in encrypted form and, on he other hand, references a list of user programs that has been licensed to the user by the manufacturer as a result of the purchase.

In Figure 1, step 10, the installation program is loaded on the data processing system of the user and is started. The installation program contains a menu prompt and asks for the input of the copy protection identification KI given to the user, of the user identification AI and of the product identification PI (step 12). A check is carried out in step 14 to see whether the copy protection identification KI_E that has been input coincides with the copy protection identification KI_D contained in the dongle. When this is not the case, then a branch to the right is made is step 14 and the program execution is aborted.

An authentification of the installation program and of the key program ensues in a following step 16, i.e. a check is carried out to see whether the installation program originally contained on the storage medium and the key program are allowed to mutually call one another. The authentification ensues, for example, according to the challenge-response principle, which represents a standard

method for the protection of programs. When the authentification proceeds successfully, a branch is made to step 18; otherwise, a program abort follows. The sequence of the steps can also be such that step 16 is run first and step 14 thereafter.

In step 18, the encrypted product identification PI that, for example, has been encrypted according to the high-compression Huffmann-Baum method is deciphered. The user identification AT given to the user is used as the key in this deciphering. The result of the deciphering step 18 is that the copy protection identification KI_{PI} and the list of user programs wanted by the user is obtained.

In the following step 20, this list of the user programs is checked for plausibility, i.e. a determination can be made as to whether the correct user programs are present. Additionally, a checksum check of the list ensues in order to prevent au unauthorized expansion of the license on the part of the customer (signature function).

In step 12, the copy protection identification KI_{PI} contained in the product identification PI is compared to the copy protection identification KI_D of the dongle of the data processing system. One proceeds to the next step 24 given coincidence. Otherwise, the program execution is aborted. In step 24, the user can again make a selection from the list of user programs he requested, for example select those user programs that are minimally needed for handling a specific job.

In the following step 26, datafiles that are needed for the user programs and their running are established in the data processing system. The key program enters the copy protection identification KI into predetermined memory areas for the selected user programs. The installation of the user programs has thus been ended in step 28.

When running the user programs, the copy protection identification KI contained in the respective user program is compared to the copy protection identification KI_D of the dongle, as is traditional. The user program is run by the data processing system only given coincidence.

As can be seen, advantages derive both at the producer side as well as at the user side. The producer can store a plurality of user programs on the available storage medium, for example all user programs that are made available to users. Thus, the producer need not write a new storage medium dependent on the order of a specific user; rather, a limitation can be made to a single storage medium or to a few storage media. The outlay for offering storage media is lowered in this way. A similar advantage derives on the part of the user. The user, upon delivery, receives a plurality of user programs from which the user can enable precisely those that the user had ordered and purchased. When the user would like to purchase another user program at a later time, then the only thing required is the enable of this user program, which already exists, by handing over a new product identification PI. The user identification AI can remain the same. The installation itself is simple and only requires a short time. The delivery of a new dongle or of a new storage medium is not required in many cases.

The executive sequence shown in Figure 1 can be modified in many respects. For example, the user programs can also be kept on hand in a central storage medium that the user can access with the Internet. Another modification provides that, after a number of user programs have been offered to the user, these are only partly enabled and activated for demonstration purposes of user programs that were not ordered. The user can then see the advantage of such further user programs and potentially order them, whereby a new storage medium for example a new CDROM, need not be sent.

On the basis of a flowchart, Figure 2 shows the advantages of the method when a new user, who does not yet have access to the storage medium with the user programs, orders user programs (block 30) and is licensed therefor by the producer. The producer defines the user data, i.e. a user identification AI and a product identification PI are produced; further, a dongle with a copy protection identification KI is offered (block 32). The data are stored (block 34) in a data bank. The user is provided with the user data, i.e. the dongle, the copy protection identification KI, the product identification PI and the user identification AI. Further, the user is provided with a CDROM on which a plurality of user programs is stored (block 36). The installation of the user programs selected by the user ensues at the user according to the executive sequence steps according to Figure 1 (block 38).

Figure 3 shows the executive sequence when an old user, who already has a CDROM with the plurality of user programs, a dongle, a copy protection identification KI and a user identification AI, orders user programs (block 40). The producer defines the user data (block 42), i.e. the product identification PI (block 44). The user identification AI can remain the same. The corresponding data are stored in the data bank (block 46). The user data are given to the user (block 48). The installation of the user programs ensues according to the method steps (block 50) indicated in Figure 1.

Although other modifications and changes may be suggested by those skilled in the art, it is the intention of the inventors to embody within the patent warranted hereon all changes and modifications as reasonably and properly come within the scope of their contribution to the art.

In the Claims:

Amend the claims as follows:

We claim:

1. A method for operating a data processing system with copy protection for user programs, comprising the steps of:

directly connecting the data processing system to a copy protection identification via a hardware module,

providing a plurality of application programs as well as an installation program and a cryptoprogram on a storage medium intended for the user,

communicating a user identification that identifies the user, an encrypted product identification that references at least one user program and a copy protection identification to the user, the communicated copy protection identification corresponding to the copy protection identification connected via the hardware module,

when processing the installation program on the data processing system, inputting the communicated copy protection identification, the user identification and the product identification, providing each user program with a predetermined memory area into which the copy protection identification can be entered,

comparing by the installation program the copy protection identification that has been input to the copy protection identification connected with the hardware module and,

given coincidence, deciphering the encrypted product identification upon utilization of the user identification as key, and

identifying the user program referenced in the product identification,

loading the selected user program from the storage medium into a memory area of the data processing system,

entering by the cryptoprogram the copy protection identification into the predetermined memory area of the selected user program, and

before running the selected application program, comparing the copy protection identification contained in the predetermined memory area to the copy protection identification directly connected with the data processing system via the hardware module, and

running the user program only given coincidence.

2. A method according to claim 1, wherein,

when running the installation program, further running of the installation program is only continued after the comparison of the copy protection identification that has been input to the copy protection identification connected with the data processing system given coincidence.

3. A method according to claim 1, wherein the product identification also contains the copy protection identification, and further comprising the step of:

comparing said copy protection identification to the copy protection identification connected with the data processing system, and

continuing running of the further program steps only given coincidence.

4. A method according to claim 1, further comprising the steps of:

referencing a plurality of application programs in said product identification;

determining a list of said application programs upon decipherment of the product identification; and

checking said list for correctness.

5. A method according to claim 4 , wherein said step of checking said list for correctness ensues on a basis of a checksum check.

6. A method according to claim 1, further comprising the step of:

accepting a user selection from the application programs of the list; and

loading only the selected application programs from the storage medium into the memory area of the data processing system.

7. A method according to claim 1, further comprising the step of:

undertaking an authentification between the installation program and the key program when the key program is called.

8. A method according to claim 7, wherein said authentification is implemented according to a challenge-response protocol.

9. A method according to claim 1, wherein product identification is compressed according to a static Huffman-Baum method.

10. A method according to claim 1, wherein the copy protection identification connected with the data processing system is situated on a hardware module that is permanently connected to the data processing system.

11. A method according to claim 10 the hardware module is a dongle that is pluggably connected to at least one of a parallel interface and a serial interface and a USB bus of the data processing system; and said dongle including the copy protection identification.

In the Abstract:

Add the new abstract as follows:

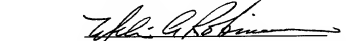
Abstract of the Disclosure

A method for operating a computer with copy protection for user programs provides that the user receives a copy protection identification, a user identification and an encrypted product identification. The product identification is decoded using the user identification as a key, so that the desired user program is determined. The key program inputs an encrypted sequence formed on the basis of the copy protection identification into a storage area of the selected user program. The user program is executed only if the copy protection identification of the computer matches the copy protection identification of the user program.

REMARKS

The foregoing amendments to the specification and claims under Article 41 of the Patent Cooperation Treaty place the application into a form for prosecution before the U.S. Patent and Trademark Office under 35 U.S.C. §371. Accordingly, entry of these amendments before examination on the merits is hereby requested.

Respectfully submitted,



Melvin A. Robinson (reg. no. 31,870)
Schiff Hardin & Waite
Patent Department
6600 Sears Tower
Chicago, Illinois 60606
Telephone: 312-258-5785

ATTORNEY FOR APPLICANT

CUSTOMER NO. 26574

Version Marked to Show Changes

The specification has been amended as follows:

SPECIFICATION

TITLE

"METHOD FOR OPERATING A DATA PROCESSING SYSTEM WITH COPY PROTECTION FOR USER PROGRAMS"

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention is directed to a method for operating a data processing system with copy protection for user programs.

Description of the Related Art

The production of user programs requires considerable development time and specific know how; it is therefore relatively involved. User programs are often loaded onto storage media, for example on CDROMs, and supplied to the user in this condition. Such storage media are relatively inexpensive and are unrelated to the economic outlay that is incurred in the production of the user program. It is not only relatively easy to make legal backup copies of such storage media with traditional data processing systems, but ~~bit~~ pirated copies of these user programs can also be easily produced and handed over to further users for a certain price or distributed in some other way. The producer of the user programs thus suffers considerable damage.

Numerous copy protection methods have been developed in order to put an ~~and~~ end to this practice. In a widespread copy protection method, a dongle is employed that is plugged onto a

parallel interface, onto a serial interface or ~~of~~ a USB bus of a data processing system. This dongle is supplied to the user together with the user program. The dongle as well as the user program contain the same copy protection identification in the form of alphanumerical characters. The presence ~~present~~ of the dongle and, thus, of the copy protection information, is queried either at the program start or continuously during the program operation. When an attempt is made to operate the user program without the dongle, then the program ~~it~~ is aborted.

When there are a great number of users who require different user programs, then a dongle is to be provided for each user. One storage medium per user must then be provided, the user programs intended for this user being contained thereon and then containing the same copy protection identification as the respective dongle. When a user orders following user programs, then the following steps are ~~respectively~~ required: producing a storage medium for this user; storing the user programs requested by the user; and providing the user programs with the copy protection identification of the dongle. Such a procedure is involved both for the user as well as for the producer of such user programs. US Patent No. ~~A~~ 5,386,369 discloses a method based on dongles.

SUMMARY OF THE INVENTION

An object of the present invention is to provide ~~offer~~ a method for operating a data processing system with copy protection for user programs that assures a dependable copy protection, works simply and can be realized with little outlay for producer and user.

According to the invention, a method for operating a data processing system with copy protection for user programs is provided ~~offered~~,

whereby a plurality of application ~~[sic]~~ programs as well as an installation program and a cryptoprogram are on hand on a storage medium,

when processing the installation program on the data processing system, the user inputs a copy protection identification, a user identification that identifies the user and an encrypted product identification that identifies at least one user program,

each user program contains a predetermined memory area into which the copy protection identification can be entered,

the installation program compares the copy protection identification that has been input to a copy protection identification connected with the data processing system and, given coincidence, deciphers the encrypted product identification upon utilization of the user identification as a key, and identifies the user program selected in the product identification,

~~that [sic]~~ the selected user program is loaded from the storage medium into a memory area of the data processing system,

the cryptoprogram enters the copy protection identification into the predetermined memory area of the selected user program, and ~~whereby,~~

before the running of the selected user program, the copy protection identification contained in the predetermined memory area is compared to the copy protection identification connected with the data processing system, and the user program is run only given coincidence.

According to the present invention, a product identification and a user identification are communicated to the user. The product identification, preferably composed of alphanumerical characters, identifies -- in encrypted form -- the user program or, respectively, a plurality of user programs purchased by the user. Further, the user ~~contains [sic] the user~~ identification is [,] likewise, for example, in the form of alphanumerical characters. This user identification serves as the key for the encryption and deciphering of the ~~said~~ product identification. With the assistance of this product

identification and the user identification, only those programs that are referenced in the product identification are enabled for the user. Accordingly, one storage medium, for example a CDROM, can contain all user programs of the manufacturer of the user programs. The customer or, respectively, user, however, can only access those user programs that he actually ordered and purchased and that can be enabled for him. The copy protection with the assistance of the copy protection identification is retained, i.e. the data processing system on which the user program is run is directly connected to a copy protection identification with the assistance of a hardware module. This user program can only be run on the specified data processing system when the user program also contains this copy protection identification; otherwise, operations are aborted. In this way, even the production of pirated copies and their forwarding to other users are ~~is [sic]~~ worthless, since this other user does not possess the matching user identification, the matching product identification and the matching copy protection identification.

In one exemplary embodiment of the invention, the product identification also contains the copy protection identification, whereby this copy protection identification is also compared to the copy protection identification connected with the data processing system, and the running of the further program steps only continues given coincidence. Usually, the copy protection identification is assigned only once. Accordingly, a copy protection for the user programs themselves is still present even if the product identification is improperly handed over to another user.

An authentification between the installation program and the key program is preferably undertaken when calling the key program, which enters the copy protection identification in predetermined memory areas of the user program. In this way, a traditional, modular key program that usually runs on standard data processing systems can be employed. Nonetheless, a protection

of the key program ensues due to the authentification between key program and installation program, and an adequate protection against misuse is established.

BRIEF DESCRIPTION OF THE DRAWINGS

An exemplary embodiment of the invention is explained below on the basis of the drawings. ~~Shown therein are:~~

Figure 1 is a flowchart that shows critical steps of the inventive method;

Figure 2 is the flowchart when a new user orders one or more user programs; and

Figure 3 shows the executive sequence when an old user orders user programs.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 shows the critical steps of the method on the basis of a simple flowchart. The customer or user receives a plurality of user programs from the manufacturer of these user programs on a storage medium, for example a CDROM, according to the order. The user, for example, has only ordered a specific selection of user programs and only paid for these. Nonetheless, many other user programs, which could be of use to the user in future and of which he can definitely make security copies, are on this storage medium. Further, the user receives a dongle from the manufacturer with a copy protection identification KI_D. This dongle must be plugged onto the parallel interface of the data processing system in order to be able to run the installation program and enable a proper operation of the user program, which has yet to be installed. Further, the user receives an alphanumerical user identification AI. This user identification serves later as the key for deciphering the product identification PI that is likewise given to the user. This product identification PI, for example, is likewise composed of alphanumerical characters and contains, on the one hand, the copy protection identification KI in encrypted form and, on he other hand,

references a list of user programs that has ~~[sic]~~ been licensed to the user by the manufacturer as a result of the purchase.

In Figure 1, step 10, the installation program is loaded on the data processing system of the user and is started. The installation program contains a menu prompt and asks for the input of the copy protection identification KI given to the user, of the user identification AI and of the product identification PI (step 12). A check is carried out in step 14 to see whether the copy protection identification KI_E that has been input coincides with the copy protection identification KI_D contained in the dongle. When this is not the case, then a branch to the right is made is step 14 and the program execution is aborted.

An authentification of the installation program and of the key program ensues in a following step 16, i.e. a check is carried out to see whether the installation program originally contained on the storage medium and the key program are allowed to mutually call one another. The authentification ensues, for example, according to the challenge-response principle, which represents a standard method for the protection of programs. When the authentification proceeds successfully, a branch is made to step 18; otherwise, a program abort follows. The sequence of the steps can also be such that step 16 is run first and step 14 thereafter.

In step 18, the encrypted product identification PI that, for example, has been encrypted according to the high-compression Huffmann-Baum method is deciphered. The user identification AT given to the user is used as the key in this deciphering. The result of the deciphering step 18 is that the copy protection identification KI_{PI} and the list of user programs wanted by the user is obtained.

In the following step 20, this list of the user programs is checked for plausibility, i.e. a determination can be made as to whether the correct user programs are present. Additionally, a checksum check of the list ensues in order to prevent au unauthorized expansion of the license on the part of the customer (signature function).

In step 12, the copy protection identification KI_{PI} contained in the product identification PI is compared to the copy protection identification KI_D of the dongle of the data processing system. One proceeds to the next step 24 given coincidence. Otherwise, the program execution is aborted. In step 24, the user can again make a selection from the list of user programs he requested, for example select those user programs that are minimally needed for handling a specific job.

In the following step 26, datafiles that are needed for the user programs and their running are established in the data processing system. The key program enters the copy protection identification KI into predetermined memory areas for the selected user programs. The installation of the user programs has thus been ended in step 28.

When running the user programs, the copy protection identification KI contained in the respective user program is compared to the copy protection identification KI_D of the dongle, as is traditional ~~traditionally~~. The user program is run by the data processing system only given coincidence.

As can be seen, advantages derive both at the producer side as well as at the user side. The producer can store a plurality of user programs on the available storage medium, for example all user programs that are made available to users. Thus, the producer need not write a new storage medium dependent on the order of a specific user; rather, a limitation can be made to a single storage medium or to a few storage media. The outlay for offering storage media is lowered in this way. A similar

advantage derives on the part of the user. The user, upon delivery, receives a plurality of user programs from which the user can enable precisely those that the user had ordered and purchased. When the user would like to purchase another user program at a later time, then the only thing required is the enable of this user program, which already exists, by handing over a new product identification PI. The user identification AI can remain the same. The installation itself is simple and only requires a short time. The delivery of a new dongle or of a new storage medium is not required in many cases.

The executive sequence shown in Figure 1 can be modified in many respects. For example, the user programs can also be kept on hand in a central storage medium that the user can access with the Internet. Another modification provides that, after a number of user programs have been offered to the user, these are only partly enabled and activated for demonstration purposes of user programs that were not ordered. The user can then see the advantage of such further user programs and potentially order them, whereby a new storage medium for example a new CDROM, need not be sent.

On the basis of a flowchart, Figure 2 shows the advantages of the ~~said~~ method when a new user, who does not yet have access to the storage medium with the user programs, orders user programs (block 30) and is licensed therefor by the producer. The producer defines the user data, i.e. a user identification AI and a product identification PI are produced; further, a dongle with a copy protection identification KI is offered (block 32). The ~~Said~~ data are stored (block 34) in a data bank. The user is provided with the user data, i.e. the dongle, the copy protection identification KI, the product identification PI and the user identification AI. Further, the user is provided with a CDROM on which a plurality of user programs is stored (block 36). The installation of the user

programs selected by the user ensues at the user according to the executive sequence steps according to Figure 1 (block 38).

Figure 3 shows the executive sequence when an old user, who already has a CDROM with the plurality of user programs, a dongle, a copy protection identification KI and a user identification AI, orders user programs (block 40). The producer defines the user data (block 42), i.e. the product identification PI (block 44). The user identification AI can remain the same. The corresponding data are stored in the data bank (block 46). The user data are given to the user (block 48). The installation of the user programs ensues according to the method steps (block 50) indicated in Figure 1.

Although other modifications and changes may be suggested by those skilled in the art, it is the intention of the inventors to embody within the patent warranted hereon all changes and modifications as reasonably and properly come within the scope of their contribution to the art.

~~List of Reference Characters~~

~~10 through 28 method steps~~

~~30 through 50 blocks~~

~~KI copy protection identification~~

~~KI_D copy protection identification in the dongle~~

~~KI_E the copy protection identification input by the user~~

~~KI_{PI} the copy protection identification contained in the product identification PI~~

~~AI user identification~~

~~PI product identification~~

The claims have been amended as follows:

Amend the claims as follows:

We claim: ~~Claims~~

1. A method Method for operating a data processing system with copy protection for user programs, comprising the steps of: ~~whereby~~

directly connecting the data processing system ~~can be directly connected~~ to a copy protection identification ~~(KI_D)~~ via a hardware module, ~~comprising the following steps:~~

~~(a)~~ providing a plurality of application ~~[sic]~~ programs as well as an installation program and a cryptoprogram ~~are on hand~~ on a storage medium ~~(CDROM)~~ intended for the user,

~~(b)~~ communicating a user identification ~~(AI)~~ that identifies the user, an encrypted product identification ~~(PI)~~ that references at least one user program and a copy protection identification ~~(KI_E) are communicated~~ to the user, ~~whereby~~ the communicated copy

protection identification corresponding ~~(KI$_E$) corresponds~~ to the copy protection identification ~~(KI$_B$)~~ connected via the hardware module,

~~(c)~~ when processing the installation program on the data processing system, inputting the communicated copy protection identification ~~(KI$_E$)~~, the user identification ~~(AI)~~ and the product identification ~~(PI) are input~~,

~~(c1)~~ providing each user program with ~~contains~~ a predetermined memory area into which the copy protection identification ~~(KI)~~ can be entered,

~~(c2)~~ comparing by the installation program ~~compares~~ the copy protection identification ~~(KI$_E$)~~ that has been input to the copy protection identification ~~(KI$_B$)~~ connected with the hardware module and,

given coincidence, deciphering ~~deciphers~~ the encrypted product identification ~~(PI)~~ upon utilization of the user identification ~~(AI)~~ as key, and

identifying ~~identifies~~ the user program referenced in the product identification ~~(PI)~~,

~~(c3)~~ loading the selected user program ~~is loaded~~ from the storage medium ~~(CDROM)~~ into a memory area of the data processing system,

~~(c4)~~ entering by the cryptoprogram ~~enters~~ the copy protection identification ~~(KI)~~ into the predetermined memory area of the selected user program, and ~~whereby~~

~~(d)~~ before ~~the~~ running ~~of~~ the selected application ~~[sic]~~ program, comparing the copy protection identification ~~(KI)~~ contained in the predetermined memory area ~~is compared~~ to the copy protection identification ~~(KI$_B$)~~ directly connected with the data processing system via the hardware module, and

running the user program ~~is run~~ only given coincidence.

2. A method ~~Method~~ according to claim 1, wherein ~~characterized in that,~~ when running the installation program, further running of the installation program is only continued after the comparison of the copy protection identification ~~(KI_E)~~ that has been input to the copy protection identification ~~(KI_D)~~ connected with the data processing system given coincidence.

3. A method ~~Method~~ according to claim 1 ~~or 2~~, wherein ~~characterized in that~~ the product identification ~~(PI)~~ also contains the copy protection identification ~~(KI_D)~~, and further comprising the step of:

comparing said ~~in that this~~ copy protection identification ~~(KI_D) is compared~~ to the copy protection identification ~~(KI_D)~~ connected with the data processing system, and ~~the~~ continuing running of the further program steps ~~is continued~~ only given coincidence.

4. A method ~~Method~~ according to claim 1, further comprising the steps of:

referencing ~~one of the preceding claims, characterized in that the product identification (PI) references~~ a plurality of application ~~[sic]~~ programs in said product identification; ~~in that~~ determining a list of said ~~these~~ application ~~[sic]~~ programs ~~is determined~~ upon decipherment of the product identification ~~(PI)~~; and ~~in that this~~ checking said list ~~is checked~~ for correctness.

5. A method ~~Method~~ according to claim 4 ~~1~~, wherein said step of checking said ~~characterized in that the check of the~~ list for correctness ensues on a ~~the~~ basis of a checksum check.

6. A method ~~Method~~ according to claim 1, further comprising the step of: ~~one of the preceding claims, characterized in that the~~

accepting a user ~~makes a~~ selection from the application ~~[sic]~~ programs of the list; and ~~in that~~

loading only the selected application ~~[sic]~~ programs ~~are loaded~~ from the storage medium into the memory area of the data processing system.

7. A method ~~Method~~ according to claim 1, further comprising the step of: ~~one of the preceding claims, characterized in that~~

undertaking an authentification between the installation program and the key program ~~is undertaken~~ when the key program is called.

8. A method ~~Method~~ according to claim 7, wherein said ~~characterized in that the~~ authentification is implemented according to a ~~the known~~ challenge-response protocol.

9. A method ~~Method~~ according to claim 1, wherein [one of the preceding claims, characterized in that the] product identification is compressed according to a [the] static Huffman-Baum method.

10. A method ~~Method~~ according to claim 1, wherein ~~one of the preceding claims, characterized in that~~ the copy protection identification ~~(KI_p)~~ connected with the data processing system is situated on a hardware module that is permanently connected to the data processing system.

11. ~~Method~~ according to claim 10 ~~11 [sic], characterized in that~~ the hardware module is a dongle that is pluggably connected to at least one of a parallel interface and ~~or to~~ a serial interface and ~~or to~~ a USB bus of the data processing system; and said ~~in that this~~ dongle including ~~contains~~ the copy protection identification ~~(KI_p).~~

The new abstract has been added as follows:

Abstract of the Disclosure

A method for operating a computer with copy protection for user programs provides that the user receives a copy protection identification, a user identification and an encrypted product identification. The product identification is decoded using the user identification as a key, so that the desired user program is determined. The key program inputs an encrypted sequence formed on the basis of the copy protection identification into a storage area of the selected user program. The user program is executed only if the copy protection identification of the computer matches the copy protection identification of the user program.

METHOD FOR OPERATING A DATA PROCESSING SYSTEM WITH COPY PROTECTION FOR USER PROGRAMS

The invention is directed to a method for operating a data processing system with copy protection for user programs.

The production of user programs requires considerable development time and specific know how; it is therefore relatively involved. User programs are often loaded onto storage media, for example on CDROMs, and supplied to the user in this condition. Such storage media are relatively inexpensive and are unrelated to the economic outlay that is incurred in the production of the user program. It is not only relatively easy to make legal backup copies of such storage media with traditional data processing systems, bit pirated copies of these user programs can also be easily produced and handed over to further users for a certain price or distributed in some other way. The producer of the user programs thus suffers considerable damage.

Numerous copy protection methods have been developed in order to put and end to this practice. In a widespread copy protection method, a dongle is employed that is plugged onto a parallel interface, onto a serial interface of a USB bus of a data processing system. This dongle is supplied to the user together with the user program. The dongle as well as the user program contain the same copy protection identification in the form of alphanumerical characters. The present of the dongle and, thus, of the copy protection information, is queried either at the program start or continuously during the program operation. When an attempt is made to operate the user program without dongle, then it is aborted.

When there are a great number of users who require different user programs, then a dongle is to be provided for each user. One storage medium per user must then be provided, the user programs intended for this user being contained thereon and then containing the same copy protection identification as the respective dongle. When a user orders following user programs, then the following steps are respectively required: producing a storage medium for this user; storing the user programs requested by the user; providing the user programs with the copy protection

identification of the dongle. Such a procedure is involved both for the user as well as for the producer of such user programs. US-A-5,386,369 discloses a method based on dongles.

An object of the invention is to offer a method for operating a data processing system with copy protection for user programs that assures a dependable copy protection, works simply and can be realized with little outlay for producer and user.

According to the invention, a method for operating a data processing system with copy protection for user programs is offered,
whereby a plurality of application [sic] programs as well as an installation program and a cryptoprogram are on hand on a storage medium,
when processing the installation program on the data processing system, the user inputs a copy protection identification, a user identification that identifies the user and an encrypted product identification that identifies at least one user program,
each user program contains a predetermined memory area into which the copy protection identification can be entered,
the installation program compares the copy protection identification that has been input to a copy protection identification connected with the data processing system and, given coincidence, deciphers the encrypted product identification upon utilization of the user identification as key, and identifies the user program selected in the product identification, that [sic] the selected user program is loaded from the storage medium into a memory area of the data processing system,
the cryptoprogram enters the copy protection identification into the predetermined memory area of the selected user program,
and whereby, before the running of the selected user program, the copy protection identification contained in the predetermined memory area is compared to the copy protection identification connected with the data processing system, and the user program is run only given coincidence.

According to the invention, a product identification and a user identification are communicated to the user. The product identification, preferably composed of alphanumerical characters, identifies -- in encrypted form -- the user

program or, respectively, a plurality of user programs purchased by the user. Further, the user contains [sic] the user identification, likewise, for example, in the form of alphanumerical characters. This user identification serves as key for the encryption and deciphering of said product identification. With the assistance of this product identification and the user identification, only those programs that are referenced in the product identification are enabled for the user. Accordingly, one storage medium, for example a CDROM, can contain all user programs of the manufacturer of the user programs. The customer or, respectively, user, however, can only access those user programs that he actually ordered and purchased and that can be enabled for him. The copy protection with the assistance of the copy protection identification is retained, i.e. the data processing system on which the user program is run is directly connected to a copy protection identification with the assistance of a hardware module. This user program can only be run on the specified data processing system when the user program also contains this copy protection identification; otherwise, operations are aborted. In this way, even the production of pirated copies and their forwarding to other users is [sic] worthless, since this other user does not possess the matching user identification, the matching product identification and the matching copy protection identification.

In one exemplary embodiment of the invention, the product identification also contains the copy protection identification, whereby this copy protection identification is also compared to the copy protection identification connected with the data processing system, and the running of the further program steps only continues given coincidence. Usually, the copy protection identification is assigned only once. Accordingly, a copy protection for the user programs themselves is still present even if the product identification is improperly handed over to another user.

An authentification between the installation program and the key program is preferably undertaken when calling the key program, which enters the copy protection identification in predetermined memory areas of the user program. In this way, a traditional, modular key program that usually runs on standard data processing systems can be employed. Nonetheless, a protection of the key program ensues due to

the authentification between key program and installation program, and an adequate protection against misuse is established.

An exemplary embodiment of the invention is explained below on the basis of the drawing. Shown therein are:

Figure 1 a flowchart that shows critical steps of the inventive method;

Figure 2 the flowchart when a new user orders one or more user programs; and

Figure 3 the executive sequence when an old user orders user programs.

Figure 1 shows the critical steps of the method on the basis of a simple flowchart. The customer or user receives a plurality of user programs from the manufacturer of these user programs on a storage medium, for example a CDROM, according to the order. The user, for example, has only ordered a specific selection of user programs and only paid for these. Nonetheless, many other user programs, which could be of use to the user in future and of which he can definitely make security copies, are on this storage medium. Further, the user receives a dongle from the manufacturer with a copy protection identification KI_D. This dongle must be plugged onto the parallel interface of the data processing system in order to be able to run the installation program and enable a proper operation of the user program, which has yet to be installed. Further, the user receives an alphanumerical user identification AI. This user identification serves later as key for deciphering the product identification PI that is likewise given to the user. This product identification PI, for example, is likewise composed of alphanumerical characters and contains, on the one hand, the copy protection identification KI in encrypted form and, on he other hand, references a list of user programs that has [sic] been licensed to the user by the manufacturer as a result of the purchase.

In Figure 1, step 10, the installation program is loaded on the data processing system of the user and is started. The installation program contains a menu prompt and asks for the input of the copy protection identification KI given to the user, of the user identification AI and of the product identification PI (step 12). A check is carried out in step 14 to see whether the copy protection identification KI_E that has been input coincides with the copy protection identification KI_D contained in

the dongle. When this is not the case, then a branch to the right is made is step 14 and the program execution is aborted.

An authentification of the installation program and of the key program ensues in a following step 16, i.e. a check is carried out to see whether the installation program originally contained on the storage medium and the key program are allowed to mutually call one another. The authentification ensues, for example, according to the challenge-response principle, which represents a standard method for the protection of programs. When the authentification proceeds successfully, a branch is made to step 18; otherwise, a program abort follows. The sequence of the steps can also be such that step 16 is run first and step 14 thereafter.

In step 18, the encrypted product identification PI that, for example, has been encrypted according to the high-compression Huffmann-Baum method is deciphered. The user identification AT given to the user is used as key in this deciphering. The result of the deciphering step 18 is that the copy protection identification KI_{PI} and the list of user programs wanted by the user is obtained.

In the following step 20, this list of the user programs is checked for plausibility, i.e. a determination can be made as to whether the correct user programs are present. Additionally, a checksum check of the list ensues in order to prevent au unauthorized expansion of the license on the part of the customer (signature function).

In step 12, the copy protection identification KI_{PI} contained in the product identification PI is compared to the copy protection identification KI_D of the dongle of the data processing system. One proceeds to the next step 24 given coincidence. Otherwise, the program execution is aborted. In step 24, the user can again make a selection from the list of user programs he requested, for example select those user programs that are minimally needed for handling a specific job.

In the following step 26, datafiles that are needed for the user programs and their running are established in the data processing system. The key program enters the copy protection identification KI into predetermined memory areas for the selected user programs. The installation of the user programs has thus been ended in step 28.

When running the user programs, the copy protection identification KI contained in the respective user program is compared to the copy protection identification KI_D of the dongle, as traditionally. The user program is run by the data processing system only given coincidence.

As can be seen, advantages derive both at the producer side as well as at the user side. The producer can store a plurality of user programs on the available storage medium, for example all user programs that are made available to users. Thus, the producer need not write a new storage medium dependent on the order of a specific user; rather, a limitation can be made to a single storage medium or to a few storage media. The outlay for offering storage media is lowered in this way. A similar advantage derives on the part of the user. The user, upon delivery, receives a plurality of user programs from which the user can enable precisely those that the user had ordered and purchased. When the user would like to purchase another user program at a later time, then the only thing required is the enable of this user program, which already exists, by handing over a new product identification PI. The user identification AI can remain the same. The installation itself is simple and only requires a short time. The delivery of a new dongle or of a new storage medium is not required in many cases.

The executive sequence shown in Figure 1 can be modified in many respects. For example, the user programs can also be kept on hand in a central storage medium that the user can access with the Internet. Another modification provides that, after a number of user programs have been offered to the user, these are only partly enabled and activated for demonstration purposes of user programs that were not ordered. The user can then see the advantage of such further user programs and potentially order them, whereby a new storage medium for example a new CDROM, need not be sent.

On the basis of a flowchart, Figure 2 shows the advantages of said method when a new user, who does not yet have access to the storage medium with the user programs, orders user programs (block 30) and is licensed therefor by the producer. The producer defines the user data, i.e. a user identification AI and a product identification PI are produced; further, a dongle with a copy protection identification

KI is offered (block 32). Said data are stored (block 34) in a data bank. The user is provided with the user data, i.e. the dongle, the copy protection identification KI, the product identification PI and the user identification AI. Further, the user is provided with a CDROM on which a plurality of user programs is stored (block 36). The installation of the user programs selected by the user ensues at the user according to the executive sequence steps according to Figure 1 (block 38).

Figure 3 shows the executive sequence when an old user, who already has a CDROM with the plurality of user programs, a dongle, a copy protection identification KI and a user identification AI, orders user programs (block 40). The producer defines the user data (block 42), i.e. the product identification PI (block 44). The user identification AI can remain the same. The corresponding data are stored in the data bank (block 46). The user data are given to the user (block 48). The installation of the user programs ensues according to the method steps (block 50) indicated in Figure 1.

List or Reference Characters

10 through 28	method steps
30 through 50	blocks
KI	copy protection identification
KI_D	copy protection identification in the dongle
KI_E	the copy protection identification input by the user
KI_{PI}	the copy protection identification contained in the product identification PI
AI	user identification
PI	product identification

Claims

1. Method for operating a data processing system with copy protection for user programs, whereby the data processing system can be directly connected to a copy protection identification (KI_D) via a hardware module, comprising the following steps:

(a) a plurality of application [sic] programs as well as an installation program and a cryptoprogram are on hand on a storage medium (CDROM) intended for the user,

(b) a user identification (AI) that identifies the user, an encrypted product identification (PI) that references at least one user program and a copy protection identification (KI_E) are communicated to the user, whereby the communicated copy protection identification (KI_E) corresponds to the copy protection identification (KI_D) connected via the hardware module,

(c) when processing the installation program on the data processing system, the communicated copy protection identification (KI_E), the user identification (AI) and the product identification (PI) are input,

(c1) each user program contains a predetermined memory area into which the copy protection identification (KI) can be entered,

(c2) the installation program compares the copy protection identification (KI_E) that has been input to the copy protection identification (KI_D) connected with the hardware module and, given coincidence, deciphers the encrypted product identification (PI) upon utilization of the user identification (AI) as key, and identifies the user program referenced in the product identification (PI),

(c3) the selected user program is loaded from the storage medium (CDROM) into a memory area of the data processing system,

(c4) the cryptoprogram enters the copy protection identification (KI) into the predetermined memory area of the selected user program,

and whereby

(d) before the running of the selected application [sic] program, the copy protection identification (KI) contained in the predetermined memory area is compared to the copy protection identification (KI_D) directly connected with the data processing system via the hardware module, and the user program is run only given coincidence.

2. Method according to claim 1, characterized in that, when running the installation program, further running of the installation program is only continued after the comparison of the copy protection identification (KI_E) that has been input to the copy protection identification (KI_D) connected with the data processing system given coincidence.

3. Method according to claim 1 or 2, characterized in that the product identification (PI) also contains the copy protection identification (KI_{PI}), and in that this copy protection identification (KI_{PI}) is compared to the copy protection identification (KI_D) connected with the data processing system, and the running of the further program steps is continued only given coincidence.

4. Method according to one of the preceding claims, characterized in that the product identification (PI) references a plurality of application [sic] programs; in that a list of these application [sic] programs is determined upon decipherment of the product identification (PI); and in that this list is checked for correctness.

5. Method according to claim 1, characterized in that the check of the list for correctness ensues on the basis of a checksum check.

6. Method according to one of the preceding claims, characterized in that the user makes a selection from the application [sic] programs of the list; and in that only the selected application [sic] programs are loaded from the storage medium into the memory area of the data processing system.

7. Method according to one of the preceding claims, characterized in that an authentification between the installation program and the key program is undertaken when the key program is called.

8. Method according to claim 7, characterized in that the authentification is implemented according to the known challenge-response protocol.

9. Method according to one of the preceding claims, characterized in that the product identification is compressed according to the static Huffman-Baum method.

10. Method according to one of the preceding claims, characterized in that the copy protection identification (KI_D) connected with the data processing system is

situated on a hardware module that is permanently connected to the data processing system.

11. Method according to claim 11 [sic], characterized in that the hardware module is a dongle that is pluggably connected to a parallel or to a serial interface or to a USB bus of the data processing system; and in that this dongle contains the copy protection identification (KI_D)

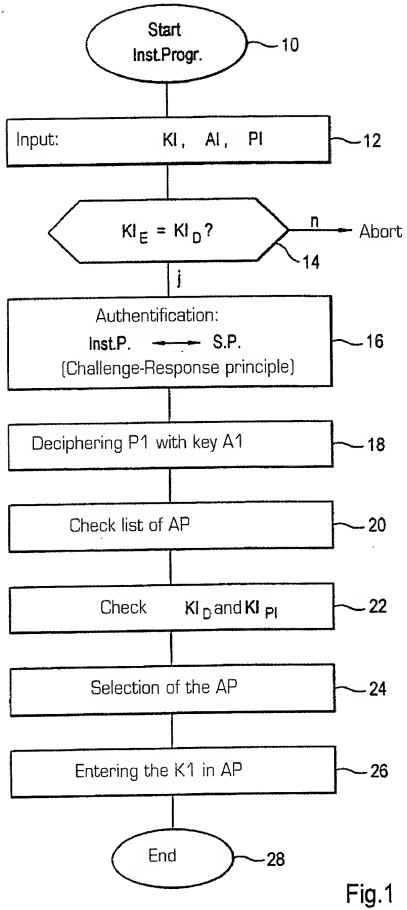

Start
Inst.Progr.
10
Input: KI, AI, PI
12
KI E = KI D ?
n
Abort
14
j
Authentification:
Inst.P. S.P.
(Challenge-Response principle)
16
Deciphering P1 with key A1
18
Check list of AP
20
Check KI D and KI PI
22
Selection of the AP
24
Entering the K1 in AP
26
End
28

Fig.1

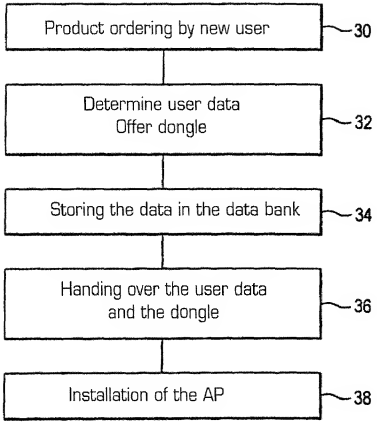


Fig.2

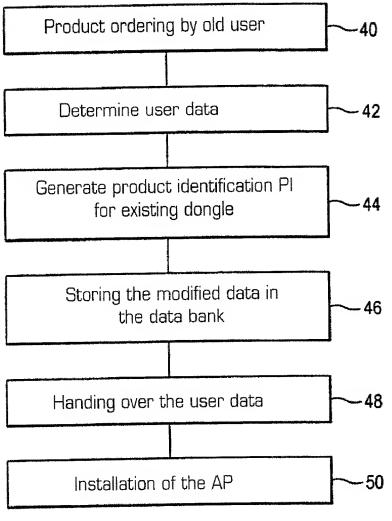

Product ordering by old user
40
Determine user data
42
Generate product identification PI for existing dongle
44
Storing the modified data in the data bank
46
Handing over the user data
48
Installation of the AP
50

Fig.3

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
ERKLÄRUNG FÜR PATENTANMELDUNGEN MIT VOLLMACHT
German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

As a below named inventor, I hereby declare that:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

My residence, post office address and citizenship are as stated below next to my name,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für des dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

VERFAHREN ZUM BETREIBEN EINER DATENVERARBEITUNGSANLAGE MIT KOPIERSCHUTZ FÜR ANWENDERPROGRAMME

deren Beschreibung

the specification of which

(zutreffendes ankreuzen)

(check one)

☐ hier beigefügt ist.

☐ is attached hereto

☒ am 4 October 1999 als PCT internationale Anmeldung PCT Anmeldungsnummer PCT/EP99/07329 eingereicht wurde und am _____ abgeändert wurde (falls tatsächlich abgeändert)

☐ was filed on _____ as PCT international application PCT Application No. _____ and was amended on _____ (if applicable)

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

German Language Declaration

Prior foreign applications
Priorität beansprucht

			Priority Claimed	
198 46 065.1	Germany	6 October 1998	■	□
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein
			□	□
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozeßordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122 I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.) (Anmeldeseriennummer)	(Filing Date) (Anmeldedatum)	(Status) (patentiert, anhängig, aufgegeben)	(Status) (patented, pending, abandoned)
(Application Serial No.) (Anmeldeseriennummer)	(Filing Date) (Anmeldedatum)	(Status) (patentiert, anhängig, aufgegeben)	(Status) (patented, pending, abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: (Name und Registrationsnummer anführen)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

And I hereby appoint all Attorneys identified by United States Patent and Trademark Office customer number 26574, who are all members of the firm of Schiff Hardin and Waite.

Telefongespräche bitte richten an: (Name und Telefonnummer)

Direct Telephone Calls to: (name and telephone number)

312/258-5785

Postanschrift:

Send Correspondence to:

SCHIFF HARDIN & WAITE
Patent Department
6600 Sears Tower, Chicago, Illinois 60606

CUSTOMER NUMBER 26574

Voller Name des einzigen oder ursprünglichen Erfinders: Hartwig SCHWIER	Full name of sole or first inventor:
Unterschrift des Erfinders: Datum 23/Jul/2001	Inventor's signature: Date
Wohnsitz: Muenchen, Germany	Residence
Staatsangehörigkeit: German	Citizenship
Postanschrift: Geisbergstrasse 8	Post Office Address
D-81675 Muenchen, GERMANY	

(Bitte entsprechende Informationen und Unterschriften im Falle von weiteren Miterfindern angeben).

(Supply similar information and signature for subsequent joint inventors).

Voller Name des zweiten Miterfinders (falls zutreffend): Thomas MATHIESEN	Full name of second joint inventor, if any:
Unterschrift des Erfinders Datum 09-07-2009	Inventor's signature Date
Wohnsitz Markt Schwaben, Germany	Residence
Staatsangehörigkeit German	Citizenship
Postanschrift Maria-Adelberger-Strasse 7 D-85570 Markt Schwaben, Germany	Post Office Address
Voller Name des dritten Miterfinders (falls zutreffend):	Full name of third joint inventor, if any:
Unterschrift des Erfinders Datum	Inventor's signature Date
Wohnsitz	Residence
Staatsangehörigkeit	Citizenship
Postanschrift	Post Office Address
Voller Name des vierten Miterfinders (falls zutreffend):	Full name of fourth joint inventor, if any:
Unterschrift des Erfinders Datum	Inventor's signature Date
Wohnsitz	Residence
Staatsangehörigkeit	Citizenship
Postanschrift	Post Office Address

(Bitte entsprechende Informationen und Unterschriften im Falle von zweiten und weiteren Miterfindern angeben).

(Supply similar information and signature for second and subsequent joint inventors).